

PRACTICE QUESTIONS

Splunk Core Certified User

SHARED BY [u/Noble-Cluster-6345](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	Splunk Core Certified User

Shared by [u/Noble-Cluster-6345](#) on aiexamcerts

10 practice questions for the Splunk Core Certified User exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/splunk/splunk-core-certified-user. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. Which index does Splunk Enterprise use by default for new data when no other index is set?

- A `_internal`
- B `main`
- C `summary`
- D `_audit`

Answer: B

The main index is the default index for data that does not name an index in its input configuration. `_internal` holds Splunk's own operational logs, and `_audit` records audit trail activity such as user searches. `summary` is used for summary index data that administrators create on purpose.

2. The default field that holds the original, unprocessed text of each event is named _____.

Answer: `_raw`

The `_raw` field holds the complete original text of each event, and fields are extracted from it at search time. Other default fields such as `_time` hold the timestamp instead. Knowing the difference helps when a regular expression needs to run against the raw text.

3. Which time modifiers select events from the last 24 hours up to the current time?

- A `earliest=24h latest=now`
- B `last=24h to=now`
- C `range=24h`
- D `earliest=-24h latest=now`

Answer: D

Relative time modifiers use a minus sign for a past offset, so `earliest=-24h latest=now` covers the last day. The value `24h` without the minus sign is not a past offset, and `last` and `range` are not search time modifiers. Syntax that looks plausible here still fails, so check the exact modifier names.

4. The host field is a default field that Splunk assigns to every event.

- A True
- B False

Answer: A (True)

Splunk assigns default fields such as host, source and sourcetype to events, usually from the originating machine and input configuration. Because host is a default field, it can be used in a search without any extraction step. Its value identifies where the event came from rather than what it contains.

5. Which two statements about Splunk search modes are correct? (Choose two.)

- A Fast mode limits field discovery so results return sooner.
- B Smart mode is the default and changes its behavior based on the type of search.
- C Verbose mode is the fastest mode and returns only summary statistics.
- D Fast mode returns only events from the _internal index.
- E Smart mode turns off field discovery for every search.

Answer: A, B

Fast mode reduces field discovery so results appear sooner, and Smart mode is the default that switches between fast and verbose behavior depending on the search. Verbose mode is the slowest because it discovers all fields and returns full events, so it is not the fastest. Fast mode does not restrict results to the _internal index, and Smart mode does not turn off field discovery for all searches.

6. Which search returns the number of events for each host value?

- A stats count by host
- B stats host count
- C table host count
- D count host

Answer: A

The stats command with count by host groups events by host and counts each group, giving one row per host. Writing stats host count omits the by keyword, so it does not produce a per-host count. table host count only displays fields and does not aggregate events.

7. Which command produces a time series of event counts in one-hour buckets, suitable for a line chart?

- A top span=1h count
- B timechart span=1h count
- C dedup _time span=1h
- D rare span=1h count

Answer: B

timechart creates a table with one row per time bucket, and span sets the bucket size, so this returns hourly counts. top and rare summarize the most and least common field values rather than time buckets. dedup removes duplicate events and does not count them.

8. A field _____ maps an existing field to a second name, so searches using either name return the same values.

Answer: alias

A field alias gives an existing field an additional name, and the values are the same under both names. Field aliases are configured as knowledge objects and are separate from calculated fields and lookups.

9. Which dashboard element lets a user select a value that filters the searches in other panels?

- A Panel title
- B Annotation
- C Lookup definition
- D Form input

Answer: D

Form inputs such as dropdowns, text boxes and time pickers let users set tokens that panel searches read. A panel title only labels a panel, an annotation adds a note, and a lookup definition maps lookup tables rather than controlling a dashboard.

10. Which knowledge object attaches a label to field values so that searches can use tag=name to match them?

- A Tag
- B Event type
- C Field alias
- D Macro

Answer: A

A tag attaches a label to field-value pairs, and searches match it with tag=name. An event type classifies events by a saved search definition and is used with eventtype=, a field alias maps one field name to another, and a macro stores reusable search text.